UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/389,540	09/03/1999	LAWRENCE SMITH	105.0163US1	5546

21186 7590 04/14/2004

SCHWEGMAN, LUNDBERG, WOESSNER & KLUTH, P.A.
P.O. BOX 2938
MINNEAPOLIS, MN 55402

EXAMINER	
VAUGHAN, MICHAEL R	

ART UNIT	PAPER NUMBER
2131	9

DATE MAILED: 04/14/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/389,540	SMITH ET AL.	
	Examiner	Art Unit	
	Michael R Vaughan	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *05 March 2004*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-17* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-17* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

Detailed Action

Response received on 3-5-04 has been fully considered. Claim 17 was added. Claims 1-17 are pending.

Response to Arguments

Applicant's arguments with respect to claims 1-9, and 17 have been considered but are moot in view of the new ground(s) of rejection.

Applicant's arguments with respect to claims 10-13 have been fully considered but they are not persuasive. Applicant argues on page 7 of the immediate response that Benson does not teach authentication of the user as described in claims 10-13. Upon further consideration of the Benson reference, the Examiner respectfully disagrees. In paragraphs [0084-0086], Benson teaches that the user is authenticated and that the Virtual Smart Card (hereinafter VSC) acts as a mediator between the user and the server. In other word the VSC assists the user to authenticate by providing the necessary functions as disclosed by Benson to prove authentication. Benson discloses that complex password authentication schemes also exist to further strengthen the authentication process [0086]. During this process and in addition to the user authentication, the VSC of the user must also be authenticated [0083] and an example

of that procedure is found in paragraphs [0049-0050]. Ultimately the whole process is designed to insure a legitimate user processes his/her legitimate VSC.

Applicant's arguments with respect to claims 14-16 have been fully considered but they are not persuasive. Applicant argues on page 8 of the immediate response that Benson nor the Handbook of Applied Cryptography (hereinafter HAC) teaches a directory service. Upon further consideration of the Benson reference, the Examiner respectfully disagrees. In paragraphs [0025-0026], Benson explicitly discloses the use of a database, which stores all of the protected information for each user of the system. Benson does not explicitly name this feature a directory service, but the functioning of the database acts like a directory service. The server is able to retrieve information based on the identity of the user to provide a service to the user, i.e. authentication. The Examiner reasserts that the teachings of HAC, the use of a digital certificate to further authenticate the public key of a user, is an obvious feature to employ within the system of Benson. Therefore, the public key of each user would also be stored in the database of Benson.

Claim Rejections - 35 USC § 103

Claims 1-6 are rejected under 35 U.S.C. 103(a) as being unpatentable over Benson (EP 936,530 A1) in view of Vilhuber (USP 6,470,453).

As per claim 1, Benson teaches:

A virtual smart card server [0049];

Storage connected to the virtual smart card server, which includes a plurality of smart card [0013];

Virtual smart cards (hereinafter VSC) are associated with a user [0013];

VSC include a private key [0007].

A virtual smart card agent connected to the virtual smart card server [0049 and 0083];

Accessing the authenticated user's VSC to obtain the user's private key [0086]. Benson fails to explicitly disclose the virtual smart card agent includes a user authentication interface for user by a user in entering a one-time pad. Benson does teach that the VSC is able to receive as input a one time random number [0049]. Benson also teaches that the weakest point of his system is the password entered by the user [0067]. Benson says that one can optionally configure a VSC server to require additional authentication material [0067] and that more complex password authentication can be used [0086]. Vilhuber teaches a more complex password authentication which is more secure. Vilhuber explicitly teaches that the user enters a one time password which is displayed on a token. In view of this, it would have been obvious to one of ordinary skill in the art at the time of the invention to employ the teachings of Vilhuber within the system of Benson because a simple password is not nearly as secure as using one time random passwords.

As per claim 17, Benson in view of Vilhuber teach displaying the one-time password on an authentication token.

As per claim 2, Benson teaches that the VSC interfaces with applications [0017].

As per claim 3, Benson teaches that the VSC performs encryption [0037] in response to applications [0023-0024].

As per claim 4, Benson teaches the VSC digitally signs a keyfile [0044].

As per claim 5, Benson teaches the VSC stores all of the protected information including key management [0025] in response to applications [0023-0024]. Benson teaches that a channel is established using key management functions [0036-0037]. It is therefore inherent that a channel is establishment after an application has detected the use of a VSC and must authenticate the VSC with the server.

As per claim 6, Benson teaches an authentication server connected to the virtual smart card agent and wherein the virtual smart card agent authenticates the user through interaction with the authentication server [0049 and 0083];

As per claim 7, Benson teaches an authentication server connected to the virtual smart card server, wherein the authentication server includes means for authenticating a user using a one-time password authentication token [0049 and 0083];

As per claim 8 and 9, Benson teaches that the VSC server communicates with the VSC over a transport layer [0036]. Benson also teaches that the VSC server communicates over the Internet [0024]. Therefore it is inherent that the VSC server uses TCP/IP to communicate with its clients because it uses a transport layer over the Internet.

Claims 10 –16 are rejected under 35 U.S.C. 103(a) as being unpatentable over Benson in view of Handbook of Applied Cryptography (HAC hereinafter).

As per claims 10, 11, and 12, Benson teaches a method of authenticating users using a one time random password, which is encrypted and later decrypted [0049-0050]. If the random password can be decrypted in a reasonable amount of time, the user is authenticated [0050]. Benson teaches this authentication method using a symmetric key system. Benson fails to teach an authentication method using public/private keys and the use of a digital certificate. HAC teaches an asymmetric authentication method whereby the users are given a pair of keys, one public and one private (pg. 559-560). Also HAC teaches the use of a digital certificate to further authenticate the public key of a user (pg. 560). HAC teaches that the digital certificate

must not be revoked (by checking a CRL) in order to pass validation (pg. 560 and pg. 576 – 577). The digital certificate is used to validate and obtain the public key of the authenticating user, which is used to decrypt data that was encrypted with the private key. HAC also teaches that one time passwords are encrypted with keys (pages 396-397). One of ordinary skill in art would know that the private key could encrypt the one time random password. In view of this, it would have been obvious to one of ordinary skill in the art at the time of the invention to employ the teachings of HAC into the system of Benson because it would allow two parties to authenticate by means of a trusted authentication protocol. Therefore the server would know that the user is legit because it can verify this by means of a trusted authority (HAC pg. 560).

As per claim 13, Benson's method is implemented in software and therefore it is inherent that a computer executes the program code necessary to carry out the method's steps [57].

As per claim 14, Benson teaches an authentication server [57] which stores keys and other important data such as digital signatures [0025-0026], which are associated to users [0025]. Benson teaches a host system whereby the server handles the authentication. Benson teaches that other components facilitate the transferring of data between the application and the server ([0023] and FIG. 1). The authentication server must in fact communicate with the other system components in order to maintain the record of who is currently using the VSC. Benson is silent in disclosing that a client

signs a digital signature. The server does keep record of digital signatures. HAC teaches that challenge-responses may be performed by digitally signing the challenge to prove knowledge of a private key (pg. 403). One who proves knowledge of a private key must also know the public key of the pair. It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the teachings of HAC into the system of Benson because the authentication server stores digital signatures and by signing challenges, the result could then be compared to the stored signatures to prove a that a user was using his/her own public key. Also HAC teaches the use of a digital certificate to further authenticate the public key of a user (pg. 560). The use of digital signatures and proving them are ways to ensure that users are whom they say they are.

As per claim 15, Benson is silent in disclosing that users have role-based access control. Having role-based access control makes a system able to have users that do not all have the same permissions and access to the same resources. Such is the case with most networks today. Some users have more permissions and are able to access more of the systems resources. Therefore, a network would want a way of differentiating between users based on the level of access. HAC teaches each resource has a list of identities associated with it (pg. 387). In view of this, it would have been obvious to one of ordinary skill in the art at the time of the invention to employ the teachings of HAC within the system of Benson because it would allow the system to allocate certain resources to particular users upon authenticating the user.

This is one reason why it is pertinent that the system can stop users pretending to be someone else from entering the system.

Benson fails to teach that authenticating is logged. HAC teaches that authenticating is one motivation to allow resource usage to be tracked to identifiable entities (pg. 387). In view of this, it would have been obvious to one of ordinary skill in the art at the time of the invention to employ the teachings of HAC within the system of Benson because it would allow the system to keep a log of all who try to authenticate the system. The log can be analyzed to see which users are abusing the system or whose identity has been stolen.

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Michael R Vaughan whose telephone number is 703-305-0354. The examiner can normally be reached on M-F 7:30-4:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 703-305-9648. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

MV
Michael R Vaughan
Examiner
Art Unit 2131

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100